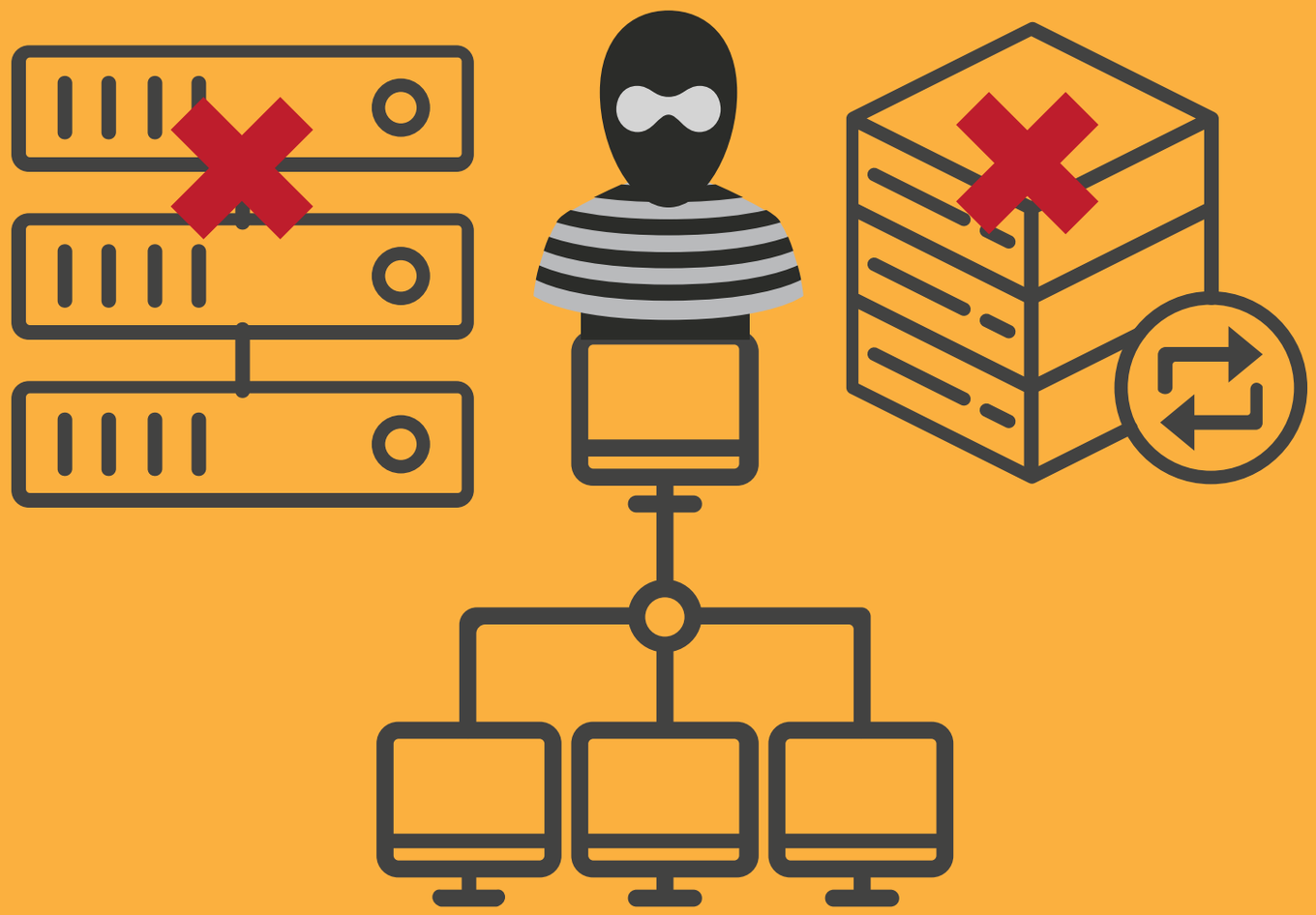
AsiaInfo | 亚信安全

某公司删库事故启示录



背景:从2月23日晚间,某互联网公司的SaaS业务生产环境和数据遭到严重破坏,直到2月25日核心业务才基本恢复,大部分业务到2月28日晚间才完全修复。

删库事件近几年发生多次,经常成为技术圈中的调侃话题。以下是部分事故记录:

1. 2018年9月,国内某快递公司数据中心的一位某工程师因误删生产数据库,导致某项服务无法使用并持续590分钟。
2. 2018年4月,VPS 服务商 Kuriko 因 rm -rf /*,宿主机上所有数据丢失。
3. 2017年9月,国内某著名IT公司的工程师帮助某运营商进行扩容割接(即增加系统容量)时,不小心将 HSS 设备里面的用户数据格式化删除,导致此运营商近 80 万用户数据丢失。

AsiaInfo | 亚信安全

此次删库事件的情况分析：

一、某集团内部应该已经构了一定的安全能力：

VPN：提供远程网络接入，提供基础的身份认证和网络访问授权。

跳板机：SaaS服务器只允许来自跳板机的访问，提供了基础的网络和数据库网络准入控制。

数据库主备：具备故障迁移时的可用性，以及数据恢复能力。

生产环境对运维权限放得较宽，对研发权限一般是收紧的。

二、删除数据具有可恢复性：

在本次事故中，主备数据均被删除。万幸是进行了「Delete」操作，而没有进行「Purge」、「覆写」、「加密毁密钥」等操作，这种情况下还能从副本或者磁盘恢复，只是恢复效率慢，时间长。

548052aaaf 90aa6333 aac1021

AsiaInfo | 亚信安全

业务风险管理措施建议

1.数据库权限管理

- 最小化权限原则
- 分库分表

2.数据库主从及备份

1）主从：当出现故障时能够进行故障迁移，满足高可用。
2）备份：实时备份：在线备份数据库进行读写分离，用于数据恢复。离线备份：日常异地离线备份，用于数据灾难恢复

目前，犯罪嫌疑人某工已经被刑事拘留，某集团的核心业务已恢复，剩余部分数据也已经在逐步恢复。「某集团事件」代表的可能是众多中小互联网企业安全建设情况的缩影，也给所有的企业敲响了警钟，内部人员作案仍然是让所有企业安防范的重点以及难点。

亚信安全技术专家总结这次事故中所暴露出来的问题，从业务风险管理的角度给出了一些针对性的建议。

AsiaInfo | 亚信安全

3.备份数据权限控制

1）设置备份数据的操作权限策略，限制高危敏感操作，如drop、rm等。
2）设置备份数据的访问控制策略，否则易导致另一种的数据泄露问题。

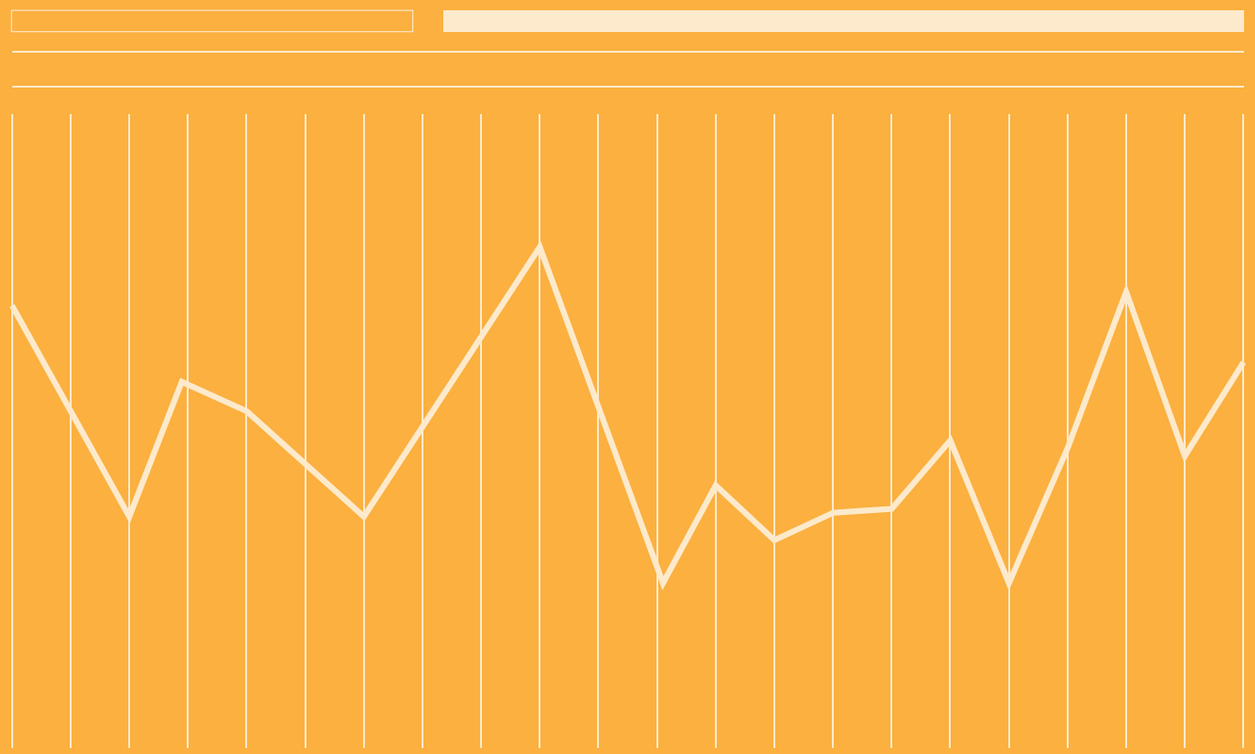
4.指令控制和审计

1）操作系统的敏感/关键指令的限制和监控，
并对操作指令历史进行采集和远程存储分析。
2）数据库审计，对数据库流量或日志审计，设定告警通知机制。

AsiaInfo | 亚信安全

5.管理流程优化改进

1）线上变更的流程审批，申请变更时段和操作细节，效率会慢一点，但提升了安全性。
2）系统性的风险评估，识别与量化风险，进行风险处置，降低风险。
3）BCP(业务连续性计划)和DRP(灾难恢复计划)的制定、评估和周期性演练。
达到一定规模体量的企业，是有必要认真考虑这两个计划。



oz10xa -40638004aa-ozx2